# Sentinel 7.3.0.1 Release Notes

May 2015




Sentinel 7.3.0.1 resolves specific previous issues. This document outlines why you should install this hotfix.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Sentinel forum on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the Sentinel NetIQ Documentation page. To download this product, see the Sentinel Product Upgrade website.



# 1 What's New?

This hotfix resolves the following issues:

## 1.1 Unable to Edit Complex Correlation Rules That Include the Trigger Operation

**Issue:** You cannot edit complex correlation rules that are in combination with one of the trigger operations, such as Window, Sequence, Distinct, or Gate operations. For example, you cannot edit PCI 8.5 Multiple User Account Access and PCI 8.5 Single User Multiple Accounts correlation rules. However, the correlation rules work as expected. (`Bug 917737)`

**Fix:** You can now edit complex correlation rules that include trigger operations.

For more information, see Creating Correlation Rules.

## 1.2 Security Vulnerability Fix

This hotfix resolves the Cross-site scripting (XSS) vulnerability in a few Sentinel components.

# 2 System Requirements

For information about hardware requirements, supported operating systems, and browsers, see the NetIQ Sentinel Technical Information Website.

# 3 Upgrading to Sentinel 7.3.0.1

You can upgrade to Sentinel 7.3.0.1 from Sentinel 7.0 or later.

Download the Sentinel installer from the NetIQ patch Finder website. For information about upgrading to Sentinel 7.3.0.1, see "Upgrading Sentinel" in the *NetIQ Sentinel Installation and Configuration Guide*.

## 3.1 Post Upgrade Configuration for Sentinel Versions Prior to 7.3

If you are upgrading to Sentinel 7.3.0.1 from a version prior to Sentinel 7.3, perform the following:

After the upgrade, the Data Proxy User role will not have the **Allow users to manage alerts** permission. This permission is necessary for the role to be able to perform remote alert search. Assign the **Allow users to manage alerts** permission to the Data Proxy User role Manually. For more information, see "Configuring Roles and Users" in the *NetIQ Sentinel Administration Guide*.

# 4 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

## 4.1 SpyEye Tracker Feeds Have Been Discontinued By Its Provider

**Issue:** The data provider for the SpyEye Tracker feed has discontinued updates to this feed, stating that the SpyEye threat appears to be mitigated. This feed plug-in is still bundled in Sentinel. Since the data provider no longer supplies valid threat feeds, the feed plug-in populates the dynamic lists with unexpected data, and related correlation rules do not work properly. The Feeds user interface only indicates that data was processed successfully, but does not indicate that the data is invalid. `(BUG 916560).`

**Workaround:** The SpyEye Tracker plug-in does not cause any issues to your server, but you can conserve system resources by removing this feed plug-in and its related Sentinel objects: dynamic list and correlation rules.

Uninstall the SpyEye Botnet component in the Solution Packs Manager. This will remove the associated dynamic lists, correlation rules, and the feed plug-in. However, if the feed plug-in was scheduled or run previously, you cannot remove the feed plug-in. Instead, you can set the schedule to update feeds to Never. For more information about removing SpyEye Botnet component in the Solution Packs Manager, see the Threat Intelligence Solution Pack documentation on the Sentinel Plug-ins Web site.

## 4.2 Tips Table Search Does Not Return the Complete List of Alert Fields in Upgraded Sentinel Installations

**Issue:** In upgraded installations of Sentinel 7.3, when you search for alert attributes in the Tips table in the Web Console, the search does not return the complete list of alert fields. However, alert fields display correctly in the Tips table if you clear the search. `(BUG 914755)`

**Workaround:** There is no workaround at this time.

## 4.3 Cannot Launch Sentinel Control Center and Solution Designer Using JRE 8 When Sentinel is in FIPS Mode

**Issue:** When the Sentinel server is running in FIPS 140-2 mode, you cannot launch Sentinel Control Center and Solution Designer in the client computer using Java Web Start if the Java Runtime Environment (JRE) version is 8 or later. `(BUG 910452)`

**Workaround:** Ensure that you perform the following in the client computer where you want to launch Sentinel Control Center or Solution Designer:

- Install and use JRE 7 to launch Sentinel Control Center or Solution Designer.
- In the Java Control Panel, do not select the **Use TLS 1.2** option in the **Advanced** tab.

## 4.4 Data Synchronization Fails While Synchronizing IPv6 Addresses in Human Readable Format

**Issue:** Data synchronization fails when you try to synchronize IPv6 address fields in a human readable format to external databases. For information about configuring Sentinel to populate the IP address fields in human readable dot notation format, see Creating a Data Synchronization Policy Creating a Data Synchronization Policy in *NetIQ Sentinel Administration Guide*. (BUG 913014)

**Workaround:** To fix this issue, manually change the maximum size of the IP address fields to at least 46 characters in the target database, and re-synchronize the database.

## 4.5 Event Search Does Not Respond if You Do Not Have Any Event Viewing Permissions

**Issue:** If run an event search when your role's security filter is blank and your role does not have event viewing permissions, the search does not complete. The search does not display any error message about the invalid event viewing permissions. (BUG 908666)

**Workaround:** Update the role with one of the following options:

1. Specify a criteria in the **Only events matching the criteria** field. If users in the role should not see any events, you can enter **NOT sev:[0 TO 5]**.
2. Select **View system events**.
3. Select **View all event data (including raw data and NetFlow data)**.

## 4.6 Sentinel Agent Manager Does Not Consider the RawDataTapFileSize Configuration

**Issue:** Sentinel Agent Manager ignores the value specified in `RawDataTapFileSize` attribute in the `SMServiceHost.exe.config` file for the raw data file size configuration, and stops writing to the raw data file when the file size reaches 10 MB. (BUG 867954)

**Workaround:** Manually copy the content of the raw data file into another file and clear it when the file size reaches 10 MB, so that Sentinel Agent Manager can write new data into it.

## 4.7 The Event fields Panel is Missing in the Schedule Page When Editing Some Saved Searches

**Issue:** When editing a saved search upgraded from Sentinel 7.2 to a later version, the **Event fields** panel, used to specify output fields in the search report CSV, is missing in the schedule page. (BUG 900293)

**Workaround:** After upgrading Sentinel, recreate and reschedule the search to view the **Event fields** panel in the schedule page.

## 4.8 Sentinel Does Not Return Any Correlated Events When You Search for Events for the Deployed Rule with the Default Fire Count Search

**Issue:** Sentinel does not return any correlated events when you search for all correlated events that were generated after the rule was deployed or enabled, by clicking the icon next to **Fire count** in the **Activity statistics** panel in the Correlation Summary page for the rule. `(BUG 912820)`

**Workaround:** Change the value in the **From** field in the Event Search page to a time earlier than the populated time in the field and click **Search** again.

## 4.9 Sentinel in FIPS Mode Does Not Display Change Guardian Delta Attached information

**Issue:** Sentinel running in FIPS mode does not display Change Guardian delta attached information when you search for Change Guardian events and click the **Change Guardian** icon, in spite of being configured to receive Change Guardian events. Change Guardian 4.1.1.1 and earlier versions do not support sending events in FIPS-compatible mode. `(BUG 912230)`

**Workaround:** There is no workaround at this time.

## 4.10 Occurrences Count Decreases After Refreshing the Alert View

**Issue:** In the alert view, the **Occurrences** count decreases when you refresh the alert view. `(BUG 913838)`

**Workaround:** Navigate to the alert summary page by clicking **View details** next to the alert for which the **Occurrences** count has decreased. The alert summary page displays the correct **Occurrences** value.

## 4.11 Data Collection and Data Synchronization With the DB2 Database Fail After Upgrading to Sentinel 7.3

**Issue:** Upgrading to Sentinel 7.3 causes data collection and data synchronization with the DB2 database to fail, because the upgrade removes the IBM DB2 JDBC driver. `(BUG 909343)`

**Workaround:** After upgrading to Sentinel 7.3, add the correct JDBC Driver and configure it for data collection and data synchronization, by performing the following steps:

1. Copy the correct version of the IBM DB2 JDBC driver (`db2jcc-*.jar`) for your version of the DB2 database in the `/opt/novell/sentinel/lib` folder.
2. Ensure that you set the necessary ownership and permissions for the driver file.
3. Configure this driver for data collection. For more information, see the Database Connector documentation.

## 4.12 New Incoming Alerts Incorrectly Appear to be Selected When You Modify Existing Alerts

**Issue:** When you click **Select All** in alerts views to select alerts, deselect few alerts, and modify them, new incoming alerts are also selected in the refreshed alert views. This results in wrong count of alerts selected for modification, and also it appears as if you are modifying new incoming alerts too. However, only the originally selected alerts are modified. `(BUG 904830)`

**Workaround:** No new alerts will appear in the alert view if you create the alert view with a custom time range.

## 4.13 Loading Historical Security Intelligence Data Takes a Long Time

**Issue:** Historical Security Intelligence (SI) data takes a long time to load in Sentinel systems that have a high Events Per Second (EPS) load. `(BUG 908599)`

**Workaround:** If you are creating a security intelligence dashboard with historical data, plan to deploy the dashboard when the load on your system is lower, if possible. There is no other workaround at this time.

## 4.14 Security Intelligence Dashboard Displays Invalid Baseline Duration When Regenerating a Baseline

**Issue:** During Security Intelligence baseline regeneration, the start and finish dates for the baseline are incorrect and display 1/1/1970. `(BUG 912009)`

**Workaround:** The correct dates are updated after the baseline regeneration is complete.

## 4.15 Sentinel Server Shuts Down When Running a Search If There Are Large Number of Events in a Single Partition

**Issue:** Sentinel server shuts down when you run a search if there are a large number of events indexed in a single partition. `(BUG 913599)`

**Workaround:** Create retention policies in such a way that there are at least two partitions open in a day. Having more than one partition open helps reduce the number of events indexed in partitions.

You can create retention policies that filter events based on the `estzhour` field, which tracks the hour of the day. Therefore, you can create one retention policy with `estzhour:[0 TO 11]` as the filter and another retention policy with `estzhour:[12 TO 23]` as the filter.

For more information, see "Configuring Data Retention Policies" in the *NetIQ Sentinel Administration Guide*.

## 4.16 Alert Roll-Up Occasionally Fails and New Alert is Created

**Issue:** A new alert is created instead of alert information rolling up to an existing alert. This is a sporadic issue. `(BUG 914512)`

**Workaround:** There is no workaround at this time.

## 4.17 Error While Using the report_dev_setup.sh Script to Configure Sentinel Ports for Firewall Exceptions on Upgraded Sentinel Appliance Installations

**Issue:** Sentinel displays an error when you use the `report_dev_setup.sh` script to configure Sentinel ports for firewall exceptions. `(BUG 914874)`

**Workaround:** Configure Sentinel ports for firewall exceptions through the following steps:

1. Open the `/etc/sysconfig/SuSEfirewall2` file.
2. Change the following line:

```
FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
40000:41000 1290 1099 2000 1024 1590"
```

to

```
FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
40000:41000 1290 1099 2000 1024 1590 5432"
```

3 Restart Sentinel.

## 4.18 Sentinel Generic Collector Performance Degrades When Generic Hostname Resolution Service Collector is Enabled

**Issue:** Sentinel Generic Collector performance degrades when Generic Hostname Resolution Service Collector is enabled on Microsoft Active Directory and Windows Collector. EPS decreases by 50% when remote Collector Managers send events. `(BUG 906715)`

**Workaround:** There is no workaround at this time.

## 4.19 Sentinel Cannot Access Security Intelligence, Netflow, and Alert Data in FIPS Mode

**Issue:** When you install Sentinel in FIPS mode, connector to Security Intelligence database fails to start, and Sentinel cannot access Security Intelligence, Netflow, and alert data. `(BUG 915241)`

**Workaround:** Restart Sentinel after installing and configuring in FIPS mode.

## 4.20 Security Intelligence Database and Alert Dashboard Occasionally Do Not Work in Upgraded Custom Installations of FIPS Enabled Sentinel

**Issue:** When you upgrade to Sentinel 7.3 from a custom installation of Sentinel that was installed by a non-root user and was configured in FIPS mode, Security Intelligence database and Alert Dashboard occasionally do not start. `(BUG 916285)`

**Workaround:** Perform the following steps:

1. Go to `<`*`custom installation directory`*`>/opt/novell/sentinel/bin` to know the Sentinel Indexing Service.
2. Run the following command:

   ```
   ./si_db.sh status
   ```

   Verify whether the following output displayed:

   ```
   Connection between alert store and indexing service is running.
   Security Intelligence database is running.
   Indexing service is running.
   ```

   If any of the above mentioned three services are not running, perform the following steps.
3. Run the following command to stop Sentinel:

   ```
   rcsentinel stop
   ```
4. Log in to the Sentinel server as the novell user.
5. Run the following command:

   ```
   <custom installation directory>/opt/novell/sentinel/bin/si_db.sh startnoauth
   ```

6 Run the following commands to add dbauser and appuser users:

```
cd <custom installation directory>/opt/novell/sentinel/3rdparty/mongodb/bin
./mongo
use admin
db.addUser ("dbauser", "novell")
use analytics
db.addUser ("appuser", "novell")
exit
```

7 Stop the MongoDB database:

```
<custom installation directory>/opt/novell/sentinel/bin/si_db.sh stop
```

8 Perform the following steps to add encrypted password fields:

8a Run the following command to get the encrypted password for the novell user:

```
<custom installation directory>/opt/novell/sentinel/bin/encryptpwd -e
novell
```

Encrypted password is displayed. For example:

```
bVWOzu6okMmMCkgM0aHeQ==
```

8b In the `configuration.properties` file, update the `baselining.sidb.password` and `baselining.sidb.dbpassword` properties with the encrypted

password. for example:

```
baselining.sidb.password=9bVWOzu6okMmMCkgM0aHeQ==
baselining.sidb.dbpassword=9bVWOzu6okMmMCkgM0aHeQ==
```

9 Exit from novell user account and start Sentinel as root user using the following command:

```
rcsentinel start
```

---

**NOTE:** Run the `configure.sh` script to reset the password whenever needed. For more information about running the `configure.sh` script, see "Modifying the Configuration after Installation" in the *NetIQ Sentinel Installation and Configuration Guide*.

---

## 4.21 Sentinel Does Not Display Trigger Events for Remote Alerts

**Issue:** In alert views, when you click **View Details** next to any remote alert and go to the Alert Details page, trigger events for that alert do not display in the **Associated Data** panel. (BUG 916116)

**Workaround:** Log in to the data source server and view the alert details locally.

## 4.22 Sentinel Does Not Display Customized Alert Properties in Alert Views for Remote Alerts

**Issue:** In alert views, **State** and **Priority** fields remote alerts display no data if the values for these fields are customized. These fields display no data in Alert Details page for the alerts too. (BUG 915762)

**Workaround:** Log in to the data source server and view the alerts locally.

## 4.23 Sometimes Sentinel Does Not Display Alerts in Alert Views After a Restart

**Issue:** Sometimes, Sentinel does not display alerts in any alert view if you restart Sentinel and log in. (BUG 916133)

**Workaround:** Restart the Security Intelligence database by performing the following steps:

1. Run the following command:

   `rm /opt/novell/sentinel/3rdparty/mongoconnector/config.txt`

2. Edit `/opt/novell/sentinel/bin/elasticsearch.sh` as follows:

   **2a** In function es_start(), enter `sleep 2` after line number 209 as shown in the following snippet:

```
 exec_command "\"${ESEC_HOME}/3rdparty/elasticsearch/bin/elasticsearch\" -
d -Des.config.file=\"${ESEC_CONFIG_HOME}/3rdparty/elasticsearch/
elasticsearch.yml\" -Des.path.conf=\"${ESEC_CONFIG_HOME}/3rdparty/
elasticsearch\" -Des.path.data=\"${ESEC_DATA_HOME}/3rdparty/elasticsearch/
data\" -Des.path.logs=\"${ESEC_LOG_HOME}/log\""
                if [ $? -ne 0 ]
                then
                        RETRY=$(( $RETRY + 1 ))
                        error_message "$(gettext 'Failed to start indexing
service.')"
                        if [ $RETRY -eq 5 ]
                        then
                        return $RESULT_FAILURE
                        fi
                        sleep 2
                        continue
                fi
                sleep 2
       fi
```

   **2b** Save the file and exit the editor.

3. Run the following command as novell user:

   `/opt/novell/sentinel/bin/si_db.sh restart`

## 4.24 Security Vulnerability in SSL 3.0

**Issue:** A vulnerability exists in SSL 3.0 that might allow plaintext of secure connections to be calculated. For more information, see CVE-2014-3566. This vulnerability exists in the bundled version of Syslog Connector 2011.1r4 since it uses the SSL protocol.

**Workaround:** The Syslog Connector version 2011.1r5 and later resolve this issue. Until it is officially released on the Sentinel Plug-ins Web site, you can download the Connector from the Previews section.

## 4.25 The Agent Manager Connector Does Not Set the Connection Mode Property in Events If the Associated Collector Supports Multiple Connection Modes

**Issue:** The Agent Manager Connector version 2011.1r3 does not set the CONNECTION_MODE property in the events if the Collector parsing the events supports multiple connection modes. (BUG 880564)

**Workaround:** The Agent Manager Connector version 2011.1r5 and later resolve this issue. Until it is officially released on the Sentinel Plug-ins Web site, you can download the Connector from the Previews section.

## 4.26 Sentinel Does Not Configure the Sentinel Appliance Network Interface By Default

**Issue:** When installing Sentinel Appliance, the network interface is not configured by default. (BUG 867013)

**Workaround:** To configure the network Interface:

1. In the Network Configuration page, click **Network Interfaces**.
2. Select the network interface and click **Edit**.
3. Select **Dynamic Address** and then select either **DHCP** or **Static assigned IP Address**.
4. Click **Next** and then **OK**.

## 4.27 The Web Browser Displays an Error When Exporting Search Results in Sentinel

**Issue:** When exporting search results in Sentinel, the Web browser might display an error if you modify the operating system language settings. (BUG 834874)

**Workaround:** To export search results properly, perform either of the following:

- While exporting the search results, remove any special characters (outside the ASCII characters) from the export filename.
- Enable UTF-8 in the operating system language settings, restart the machine, and then restart the Sentinel server.

## 4.28 Launching the Sentinel Web Console with Port Forwarding or Destination Network Address Translation Displays a Blank Page

**Issue:** When you launch the Sentinel Web Console using port forwarding or Destination Network Address Translation (DNAT), Sentinel Web Console displays a blank page. (BUG 694732)

**Workaround:** Do not use port forwarding or Destination Network Address Translation (DNAT) to launch the Sentinel Web Console.

## 4.29 Sentinel Might Display an Error When You Create or Regenerate a Baseline

**Issue:** When you create or regenerate a security intelligence baseline, Sentinel creates the baseline successfully, but displays an error message. (BUG 848067)

**Workaround:** Ignore the error message. The creation of the baseline may take several minutes.

## 4.30 Partitions Removed from Secondary Storage are Also Removed from Primary Storage

**Issue:** If the number of days of data that secondary storage can hold is less than the number of days of data that primary storage holds, Sentinel does not use the disk space in primary storage efficiently. Partitions removed from secondary storage to free up space will also be removed from primary storage. `(BUG 860888)`

**Workaround:** Allocate enough space in secondary storage to hold data for the total number of days you want to keep online (searchable).

For more information, see “Event Data” in the *NetIQ Sentinel Administration Guide*.

## 4.31 Sentinel Services Might Not Start Automatically After the Installation

**Issue:** On systems with more than 2 TB disk space, Sentinel might not start automatically after the installation. `(BUG 846296)`

**Workaround:** As a one-time activity, start the Sentinel services manually by specifying the following command:

```
rcsentinel start
```

## 4.32 Cannot Enable Kerberos Authentication in Sentinel Appliance Installations

**Issue:** In Sentinel appliance installations, if you configure Kerberos authentication in the Kerberos module, the console displays a confirmation message that the Kerberos client configuration was successful. When you view the Kerberos module again, however, the **Enable Kerberos Authentication** option is deselected. `(BUG 843623)`

**Workaround:** There is no workaround at this time.

## 4.33 Unable to Install the Remote Collector Manager If the Password Contains Special Characters

**Issue:** When you install a remote Collector Manager, if you specify a password that contains special characters, such as ‘$’, ‘”‘, ‘\’, or ‘/’, the installation fails with errors. `(BUG 812111)`

**Workaround:** Do not use special characters in the remote Collector Manager password.

## 4.34 Restarting a Remote Collector Manager Causes Some Event Sources to Lose Connection

**Issue:** When you restart a remote Collector Manager appliance, the Syslog event sources connected on the UDP port lose connection. `(BUG 795057)`

**Workaround:** There is no workaround available at this time.

## 4.35 Unable to View More Than One Report Result at a Time

**Issue:** While you wait for one report result PDF to open, particularly report results of 1 million events, if you click another report result PDF to view, the report result is not displayed. `(BUG 804683)`

**Workaround:** Click the second report result PDF again to view the report result.

## 4.36 Agent Manager Requires SQL Authentication When FIPS Mode is Enabled

**Issue:** When FIPS mode is enabled in your Sentinel environment, using Windows authentication for Agent Manager causes synchronization with the Agent Manager database to fail. `(BUG 814452)`

**Workaround:** Use SQL authentication for Agent Manager when FIPS mode is enabled in your Sentinel environment.

## 4.37 Sentinel High Availability Installation in FIPS Mode Displays an Error

**Issue:** If FIPS mode is enabled, the Sentinel High Availability installation displays the following error:

```
Sentinel server configuration.properties file is not correct. Check the
configuration file and then run the convert_to_fips.sh script again to enable FIPS
mode in Sentinel server.
```

However, the installation completes successfully. `(BUG 817828)`

**Workaround:** There is no fix or workaround available at this time. Although the installer displays the error, the Sentinel High Availability configuration works successfully in FIPS mode.

## 4.38 Sentinel High Availability Installation in Non-FIPS Mode Displays an Error

**Issue:** The Sentinel High Availability installation in non-FIPS mode completes successfully but displays the following error twice:

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments
```

`(BUG 810764)`

**Workaround:** There is no fix or workaround available at this time. Although the installer displays the error, the Sentinel High Availability configuration works successfully in non-FIPS mode.

## 4.39 Appliance Update From Versions Prior to Sentinel 7.2 Fails in WebYaST

**Issue:** Appliance update from versions prior to Sentinel 7.2 fails because the vendor for the update packages has changed from Novell to NetIQ. `(BUG 780969)`

**Workaround:** Use the zypper command to upgrade the appliance. For more information, see Upgrading the Appliance by Using zypper in the *NetIQ Sentinel Installation and Configuration Guide*.

## 4.40 Issue with Sentinel Appliance Login

**Issue:** If you specified a $ character in the password, Sentinel stores the password differently in the database depending on where the $ is placed in the password. If the password starts with the $ special character, Sentinel stores the password with a file name. If the $ character is somewhere in the middle of the password, Sentinel truncates the password to the location of the $ character. `(BUG 734500)`

**Workaround:** The actual password is stored in the `home/novell/.pgpass` file. Obtain the password from this file and then log in to Sentinel. For example, if you specified the password as abc$123, the Sentinel stores the password as abc in the `.pgpass` file. You can log in to Sentinel by specifying abc as the password.

## 4.41 Error While Installing Correlation Rules

**Issue:** Solution Manager does not install correlation rules when a correlation rule with an identical name already exists on the system. A `NullPointerException` error is logged in the console. `(BUG 713962)`

**Workaround:** Ensure that all correlation rules have a unique name.

## 4.42 Sentinel Link Action Displays Incorrect Message

**Issue:** When you execute a Sentinel Link action from the Web Console Sentinel displays a success message even though the Sentinel Link Connector integrator test failed from the Sentinel Control Center. `(BUG 710305)`

**Workaround:** There is no workaround at this time.

## 4.43 Dashboard and Anomaly Definitions with Identical Names

**Issue:** When a Security Intelligence dashboard and an anomaly definition have identical names, the dashboard link is disabled on the Anomaly Details page. `(BUG 715986)`

**Workaround:** Ensure you use unique names when creating dashboards and anomaly definitions.

## 4.44 Active Search Jobs Duration and Accessed Columns Inaccuracies

**Issue:** The Sentinel Web Console displays negative numbers in the Active Search Job Duration and Accessed columns when the Sentinel Web Console computer clock is behind the Sentinel server clock. For example, the Duration and Accessed columns display negative numbers when the Sentinel Web Console clock is set to 1:30 PM and the Sentinel server clock is set to 2:30 PM. `(BUG 719875)`

**Workaround:** Ensure the time on the computer you use to access the Sentinel Web Console is the same as or later than the time on the Sentinel server computer.

## 4.45 IssueSAMLToken Audit Event Displays Incorrect Information in the Security Intelligence Dashboard

**Issue:** When you log in to the security dashboard and perform a search for `IssueSAMLToken` audit event, the `IssueSAMLToken` audit event displays incorrect hostname (InitiatorUserName) or (IP address) SourceIP. `(BUG 870609)`

**Workaround:** There is no workaround at this time.

### 4.46 Sentinel Control Center Does Not Launch When NetIQ Identity Manager Designer is Installed on the Client Computer

**Issue:** Sentinel Control Center does not launch when the NetIQ Identity Manager Designer is installed on the client computer and Designer uses the system JRE. Designer needs to add some supporting jar files like `xml-apis.jar` to the `lib/endorsed` directory. Some of the classes in the `xml-apis.jar` file override the corresponding classes in the system JRE that is used by the Sentinel Control Center. `(BUG 888085)`

**Workaround:** Configure Designer to use its own JRE.

### 4.47 Sentinel Agent Manager Does Not Capture the Windows Insertion String Fields With Null Values

**Issue:** While collecting event data, Sentinel Agent Manager does not capture the Windows Insertion String fields with null values. `(BUG 838825)`

**Workaround:** There is no workaround at this time.

# 5 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website.

For general corporate and product information, see the NetIQ Corporate website.

For interactive conversations with your peers and NetIQ experts, become an active member of our community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

# 6 Legal Notice